REG.NO.:

SLOT: B1

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - I
FALL SEMESTER 2026-2027

Programme Name & Branch	:	**B.Tech. Computer Science and Engineering (Information Security)**
Course Code and Course Name	:	**BCSE321L and MALWARE ANALYSIS**
Faculty Name(s)	:	**Ms.Sanmuga Priya M and Dr. Sunija A P**
Class Number(s)	:	**VL2026270102597, VL2026270102592**
Date of Examination	:	**10.08.2026**
Exam Duration	:	**90 minutes** **Maximum Marks: 50**

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- Course Outcomes: (Type the CO statements covered in this question paper. Use the CO number as per the syllabus copy)
  1.Possess the skills to carry out static and dynamic malware analysis on various malware samples.
  2. Understand the executable formats, Windows internals, and APIs.
  3. Apply techniques and concepts to unpack, extract, and decrypt malware.
  4. Comprehend reverse-engineering of malware and anti-malware analysis techniques.
  5. Achieve proficiency with industry-standard malware analysis tools

Q. No	Question	M	CO	BL
1.	Explain the Portable Executable (PE) file format with a neat diagram. Discuss the significance of PE headers and major PE sections in malware analysis.	10	1	2
2.	Explain the taxonomy of malware and discuss various malware analysis techniques.	10	1	3
3.	Explain malware sandboxing and compare local and online malware sandboxing techniques.	10	1	4
4.	Illustrate the six levels of abstraction and explain how malware analysts use different abstraction levels during analysis.	10	1	2
5.	Analyze the differences between kernel-mode debugging and user-mode debugging. Discuss their features ,advantages and limitations.	10	2	4

****